

McAfee VirusScan Enterprise for Storage 1.0 Product Guide

COPYRIGHT

Copyright © 2008 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEESecurityAllianceExchange), MCAFEESecurityAllianceExchange, MCAFEESecurityAllianceExchange.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEESecurityAllianceExchange OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Introducing VirusScan Enterprise for Storage.....	4
Where to find McAfee enterprise product information.....	4
Finding release notes and documentation for McAfee enterprise products.....	5
Installing the Product.....	6
Before installing the product.....	6
System requirements.....	7
Installing the product software.....	7
Configuring Windows 2008 or different domain NetApp filer.....	8
Upgrading NetApp 7.1 to VirusScan Enterprise for Storage.....	8
Configuring Scanning of NetApp Filers.....	10
How scanning of NetApp filers works.....	10
Managing the list of file types scanned.....	11
Managing NetApp Filers.....	11
Configuring NetApp settings.....	12
Configuring Scanning of ICAP Compatible Storage Appliances.....	13
How scanning of ICAP servers works.....	13
Configuring the ICAP appliances.....	14
Configuring the list of ICAP file types scanned.....	14
Configuring ICAP settings.....	14

Introducing VirusScan Enterprise for Storage

McAfee® VirusScan® Enterprise for Storage 1.0 expands the VirusScan Enterprise 8.7i capabilities by providing remote scanning of NetApp filers and Internet Content Adaptation Protocol (ICAP) storage appliances.

VirusScan Enterprise for Storage 1.0 adds on to VirusScan Enterprise 8.7i. You can configure it from the VirusScan Console or use ePolicy Orchestrator versions 3.6.1 and 4.0 to centrally manage and enforce policies, then use queries and dashboards to track activity and detections. This guide describes how to install and configure VirusScan Enterprise for Storage.

NOTE: For information about using ePolicy Orchestrator, see its product documentation.

Contents

► [Where to find McAfee enterprise product information](#)

Where to find McAfee enterprise product information

The McAfee documentation is designed to provide you with the information you need during each phase of product implementation, from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledgebase available on McAfee ServicePortal.

Installation Phase	Setup Phase	Maintenance Phase
Before, during, and after installation. <i>Release Notes</i> - Known issues in the current release. - Issues resolved since the last release. - Last-minute changes to the product or its documentation. <i>Product Guide</i> - Preparing for, installing, and deploying software in a production environment.	Getting up-and-running with the product. <i>Product Guide and Online Help</i> - Setting up and customizing the software for your environment. <i>Online Help</i> - Managing and deploying products through ePolicy Orchestrator. - Detailed information about options in the product.	Maintaining the software. <i>Online Help</i> - Maintaining the software. - Reference information. - All information found in the product guide. <i>Knowledgebase</i> (knowledge.mcafee.com) - Release notes and documentation. - Supplemental product information. - Workarounds to known issues.

Finding release notes and documentation for McAfee enterprise products

Use this task to go to the release notes and other product documentation for McAfee enterprise products.

- 1 Go to knowledge.mcafee.com and select **Product Documentation** under **Useful links**.
- 2 Select **<Product Name> | <Product Version>** and select the required document from the list of documents.

Installing the Product

VirusScan Enterprise for Storage provides the ability to perform scanning for storage servers, such as NetApp Filers or, ICAP storage appliances connected over a network. This chapter describes the VirusScan Enterprise for Storage installation process.

Contents

- ▶ [Before installing the product](#)
- ▶ [Installing the product software](#)
- ▶ [Configuring Windows 2008 or different domain NetApp filer](#)
- ▶ [Upgrading NetApp 7.1 to VirusScan Enterprise for Storage](#)

Before installing the product

Take these actions before you start the installation process.

Task

- 1** Verify that you have the following:
 - a** A server with an installed, licensed version of VirusScan Enterprise 8.7i.
NOTE: This release of VirusScan Enterprise for Storage works only with VirusScan Enterprise 8.7i.
 - b** A supported storage solution: NetApp filer or ICAP storage appliance
- 2** Review the product release notes for:
 - Special requirements
 - Known issues
 - Last minute additions or changes
- 3** Get the installation files.
 - a** Retrieve the product .zip file from the McAfee website.
 - b** Extract the installation files from the product .zip file to a temporary location on the hard drive.

System requirements

Verify that your environment meets these system requirements before you start the installation process.

NOTE: These are minimum requirements and are not optimal for performance. They apply only to VirusScan Enterprise for Storage. You must also consider system requirements for any other products you are installing, such as VirusScan Enterprise or ePolicy Orchestrator.

NOTE: These are minimum requirements and are not optimal for performance. They apply only to VirusScan Enterprise for Storage. McAfee recommends you use a dedicated server for VirusScan Enterprise for Storage.

- **Processor** — An Intel processor or compatible architecture. McAfee recommends an Intel Pentium 4 processor running at a minimum of 2 GHz.
- **Operating system** — Install the product on any of these Microsoft Windows server (x86 or x64) platforms:
 - Windows Server 2003 Standard, with Service Pack 1 or 2
 - Windows Server 2003 Enterprise, with Service Pack 1 or 2
 - Windows Server 2003 R2
 - Windows Server 2008
- **Browser** — Microsoft Internet Explorer, version 5.0 or later.
- **Windows Installer** - Microsoft Windows Installer (MSI) version 3.1 or later.
- **Memory** — 2 GB RAM minimum. The ultimate RAM requirement depends on the number of concurrent scan requests VirusScan Enterprise for Storage is configured to service. (As a guideline figure 1MB of memory required per concurrent scan request).
- **Free disk space** — Adequate hard disk space. A complete installation occupies approximately 70 MB of disk space, keep in mind that VirusScan Enterprise for Storage's ICAP scanner places temporary files onto the system that are equal in size to the files it is being requested to scan.
- **VirusScan Enterprise 8.7i** — See the VirusScan Enterprise 8.7i documentation for system requirements.
- **ePolicy Orchestrator** — Version 3.6.1 Patch 1 or 4.0 for management and reporting.

Installing the product software

Use this task to install VirusScan Enterprise for Storage.

Task

- 1 From the temporary folder where you extracted the installation files, double-click **setup.exe**.
- 2 Click **Next**, then click **Finish** when the installation is complete.
- 3 Verify the installation using one of these methods:
 - View the VirusScan Enterprise **About** dialog box to confirm it displays the product name under **Installed Modules**
 - In the VirusScan Console view the Task list and confirm **Network Appliance Filer AV Scanner** and **ICAP AV Scanner** appear .

Configuring Windows 2008 or different domain NetApp filer

Use this task to configure VirusScan Enterprise for Storage on Windows Server 2008, or on a different domain than the domain where your NetApp filer is located. The NetApp filer uses named pipes to communicate with VirusScan Enterprise for Storage and a known NetApp filer issue requires you to perform manual steps after you have completed the VirusScan Enterprise for Storage installation.

Before you begin

Before you begin determine if you are installing VirusScan Enterprise for Storage on a Windows 2008 server or on a different domain than the NetApp Filer.

Different domain

If the server where you installed VirusScan Enterprise for Storage is on a different domain than your NetApp filer to permit the NetApp filer to communicate with VirusScan Enterprise for Storage you must add NTAPVSRQ to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes

NOTE: See <http://support.microsoft.com/kb/q126645/> for more information.

Windows Server 2008

If you install VirusScan Enterprise for Storage on a Windows Server 2008 to permit the NetApp filer to communicate with VirusScan Enterprise for Storage you might need to perform the following steps:

NOTE: Contact NetApp for other possible options for solving these known issues.

- 1 Click **Start | Administrative Tools | Local Security Policy**.
- 2 Expand **Local Policies** and click on **Security Options**.
- 3 Scroll down and open **Network access: Named Pipes that can be accessed anonymously** and add NTAPVSRQ.
- 4 You might need to enable **Network access: Let Everyone permissions apply to anonymous users**, if it is not already enabled.
- 5 Restart the Computer

Upgrading NetApp 7.1 to VirusScan Enterprise for Storage

Use this task to upgrade the VirusScan for NetApp 7.1 to VirusScan Enterprise 8.7i and McAfee VirusScan Enterprise for Storage.

Task

- 1 On the computer where VirusScan for NetApp 7.1 is installed, perform an install of VirusScan Enterprise 8.7i. The installation removes VirusScan for NetApp 7.1 and installs VirusScan Enterprise 8.7i.
- 2 On that same computer, install McAfee VirusScan Enterprise for Storage 1.0.

- 3** When the setup process detects settings from the installation of VirusScan for NetApp 7.1, you are prompted if you want to keep the previous settings. Select **Import Settings** if you want to keep these settings.

NOTE: After installing the VSESTOMD100.NAP file or ePolicy Orchestrator Extension, you must run the policy migration tool (ePOPolicyMigration.exe) to migrate your NetApp 7.1 policies.

Configuring Scanning of NetApp Filers

This section provides an overview and configuration instructions for NetApp filers used with VirusScan Enterprise for Storage.

Contents

- ▶ [How scanning of NetApp filers works](#)
- ▶ [Managing the list of file types scanned](#)
- ▶ [Managing NetApp Filers](#)
- ▶ [Configuring NetApp settings](#)

How scanning of NetApp filers works

There are three basic scanning scenarios depending on whether you are reading, writing, or copying files from or to the NetApp filer. These examples use copying as the method of accessing the files.

Scanning files copied from the filer

If the scanner-server's anti-virus service is running, and a client attempts to copy a file from the filer, these actions take place.

- The filer's operating system (Data ONTAP[®]) determines if the file needs to be scanned using these criteria:
 - The file's extension must match an extension listed in the Data ONTAP file extension list.
- Either the file must not be flagged as scanned (cached) by Data ONTAP or, if cached it must not have been modified since it was cached.
- The action taken depends on which criteria were met:
 - If the file needs to be scanned a request that includes the file's path and identification is queued to the scanner-server.

When the file is scanned, one of these actions occurs:

- If the file is clean, the filer caches the scan result and the client is allowed to copy it from the filer.
- If the file is not clean, the action that you specified on the **Actions** tab is carried out.
- If the file does not need to be scanned, the client is allowed to copy it from the filer.

Scanning files copied to filer

If the scanner-server's anti-virus service is running, and a client attempts to copy a file to the filer, these actions take place:

- The filer's operating system (Data ONTAP) determines if the file needs to be scanned using these criteria:
 - The file's extension must match an extension listed in the DATA ONTAP file extension list.
- **NOTE:** To view the extension list, type VSCAN at the DATA ONTAP command prompt.
- The file must either not be flagged as scanned (cached) by Data ONTAP, or if cached, it must not have been modified since it was cached.
- The action taken depends on which criteria were met:
 - If the file needs to be scanned, a request, that includes the file's path and identification, is queued to the scanner-server.

When the file is scanned, one of these actions occur:

- If the file is clean, the Filer caches the scan result and the client is allowed to copy it to the filer.
- If the file is not clean, the action that you specified on the **Actions** tab is carried out.
- If the file does not need to be scanned, the client is allowed to copy it to the filer.

Managing the list of file types scanned

Use this task to configure and manage the list of file types that are scanned by the VirusScan Enterprise for Storage NetApp filers.

Task

For option definitions, click **?** or **Help** in the interface.

- 1 Start NetApp configuration using either of the following:
 - From ePolicy Orchestrator 4.0, select **Systems | Policy Catalog**, select **VirusScan Enterprise for Storage 1.0.0** from the Product drop-down list, select **NetApp Policies** in the Category drop-down, select **edit** from the Actions column of the display, and select the **Scan Items** tab.
 - From the VirusScan Console, right-click **Network Appliance File AV Scanner**, select **Properties** from the drop-down list, and select the **Scan Items** tab.
- 2 Configure which file types, options, and heuristics to use when scanning the NetApp connected files.

Managing NetApp Filers

Use this task to configure and manage the list of NetApp filers connected to VirusScan Enterprise for Storage.

Task

For option definitions, click **?** or **Help** in the interface.

- 1 Start NetApp configuration using either of the following:
 - From ePolicy Orchestrator 4.0, select **Systems | Policy Catalog**, select **VirusScan Enterprise for Storage 1.0.0** from the Product drop-down list, select **NetApp Policies** in the Category drop-down, select **edit** from the Actions column of the display, and select the **Filers** tab.
 - From the VirusScan Console, right-click **Network Appliance File AV Scanner**, select **Properties** from the drop-down list, and select the **Network Appliance Filers** tab.
- 2 Configure the following:
 - Which filers or servers to protect
 - Scan settings
 - Administrator login information for the NetApp filer

Configuring NetApp settings

Configure the NetApp Filer settings.

Tab descriptions

Tab	Description
Filers	Configure which filers the scan server protects and a user account that has proper permissions (such as, Read, Write, and BackUp) to all the filers.
Scan Items	• Configure which files and file types to scan. • Scan for potential threats that resemble unwanted programs, Trojans, and macro viruses. • Scan inside archives and decode MIME-encoded files. • Enable scanning for unknown programs.
Exclusions	Configure which files and folders to exclude from scanning.
Performance	Configure scanning options to improve performance.
Actions	For threat detections: • Primary action to take when a threat is detected. • Secondary action to take on a threat detection if the first action fails. For unwanted program detections: • Primary action to take when an unwanted program is detected. • Secondary action to take on an unwanted program detection if the first action fails.
Reports	• Enable activity logging. • Specify the log file name and location. • Enable to limit the size of log file. • Specify the log file size limit. • Select the log file format. • Specify what to log besides scanning activity.

Configuring Scanning of ICAP Compatible Storage Appliances

This chapter describes the configure process for the VirusScan Enterprise for Storage used to provide remote scanning of storage appliances using the Internet Content Adaptation Protocol (ICAP).

Contents

- ▶ [How scanning of ICAP servers works](#)
- ▶ [Configuring the ICAP appliances](#)
- ▶ [Configuring the list of ICAP file types scanned](#)
- ▶ [Configuring ICAP settings](#)

How scanning of ICAP servers works

This section describes how VirusScan Enterprise for Storage scans Internet Content Adaptation Protocol (ICAP) servers.

NOTE: In the following example, the ICAP client is a Network Attached Storage (NAS) device.

The following process occurs when an ICAP client requests a file scan by VirusScan Enterprise for Storage:

- 1** The ICAP client contacts VirusScan Enterprise for Storage and requests that a specific file be scanned.
- 2** The file is transferred to a temporary location on the computer running VirusScan Enterprise for Storage, where it is scanned.
- 3** If the file is found to be a threat, the action taken depends on the following VirusScan Enterprise for Storage configuration:
 - If **Clean files automatically** is selected, any threats found cause an attempt to clean the file.
 - If the file is successfully cleaned, VirusScan Enterprise for Storage notifies the ICAP client that the file was a threat and was successfully cleaned, and VirusScan Enterprise for Storage returns the cleaned file to the ICAP client.
 - If unable to successfully clean the file, VirusScan Enterprise for Storage follows the ICAP standard by replacing the file with an HTML message stating that the original file is a threat and that it was unable to clean the file.
 - If **Continue scanning** is selected, VirusScan Enterprise for Storage notifies the ICAP client that the file is a threat, and the ICAP client then blocks access to this file.

Configuring the ICAP appliances

Use this task to configure the list of ICAP appliances scanned by the VirusScan Enterprise for Storage.

Task

For option definitions, click **?** or **Help** in the interface.

- 1 Start ICAP configuration using either of the following:
 - From ePolicy Orchestrator 4.0, select **Systems | Policy Catalog**, select **VirusScan Enterprise for Storage 1.0.0** from the Product drop-down list, select **ICAP Policies** in the Category drop-down, select **edit** from the Actions column of the display and select the **Connections and Server** tab.
 - From the VirusScan Console, right-click **ICAP AV Scanner**, select **Properties** from the drop-down list, and select the **Connections and Server** tab
- 2 Configure the following:
 - List of IP addresses where ICAP AV Scanner accepts connections
 - ICAP server configuration Bind address and port number

Configuring the list of ICAP file types scanned

Use this task to configure the list of file types scanned by the VirusScan Enterprise for Storage for ICAP servers.

Task

For option definitions, click **?** or **Help** in the interface.

- 1 Start ICAP configuration using either of the following:
 - From ePolicy Orchestrator 4.0, select **Systems | Policy Catalog**, select **VirusScan Enterprise for Storage 1.0.0** from the Product drop-down list, select **ICAP Policies** in the Category drop-down, select **edit** from the Actions column of the display, and select the **Scan Items** tab.
 - From the VirusScan Console, right-click **ICAP AV Scanner**, select **Properties** from the drop-down list, and select the **Scan Items** tab.
- 2 Configure the following:
 - Which file types to scan
 - Scanning options
 - Heuristics to use when scanning the ICAP connected files

Configuring ICAP settings

Use the following information to configure the ICAP server settings.

Tab descriptions

Tab	Description
Connections and Server	• Configure which IP addresses can accept ICAP scan requests. • Configure the bind address (the IP address of the computer where VirusScan Enterprise for Storage is installed) and port number. ICAP uses port 1344 by default.
Scan Items	• Configure which files and file types to scan. • Scan for potential threats that resemble unwanted programs, Trojans, or macro viruses. • Scan inside archives and decode MIME-encoded files. • Enable scanning of unwanted programs.
Performance	Configure scanning options to improve performance.
Actions	For threat detections: • Primary action to take when a threat is detected. • Secondary action to take on a threat detection if the first action fails. For unwanted program detections: • Primary action to take when an unwanted program is detected. • Secondary action to take on an unwanted program detection if the first action fails.
Reports	• Enable activity logging. • Specify the log file name and location. • Enable to limit the size of the log file. • Specify the log file size limit. • Select the log file format. • Specify what to log besides scanning activity.

Index

A

- Actions tab
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [12](#)
- activity logs
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [12](#)

B

- bind IP addresses and port numbers, VirusScan Enterprise for ICAP [14](#)
- browser requirements [7](#)

C

- configuration of VirusScan Enterprise for Storage
 - using ePolicy Orchestrator [4](#)
 - using VirusScan Console [4](#)
- Connections and Server tab, VirusScan Enterprise for ICAP [14](#)

D

- detections
 - unwanted programs, VirusScan Enterprise for ICAP [14](#)
 - unwanted programs, VirusScan Enterprise for NetApp [12](#)
- disk space requirements [7](#)
- documentation [4](#)

E

- ePolicy Orchestrator
 - version requirements [7](#)
- Exclusions tab, VirusScan Enterprise for NetApp [12](#)

F

- filer, VirusScan Enterprise for NetApp [11](#)
- filers
 - managing VirusScan Enterprise for NetApp [11](#)
- Filers tab, VirusScan Enterprise for NetApp [12](#)

H

- how scanning works
 - NetApps [10](#)
 - ICAP [13](#)

I

- ICAP, See Internet Content Adaptation Protocol [4](#)
- installation [6](#), [7](#)
 - system requirements [7](#)
- Internet Content Adaptation Protocol
 - defined [4](#)
 - overview [13](#)

- Internet Content Adaptation Protocol, configuring [13](#)
- IP addresses, VirusScan Enterprise for ICAP [14](#)

L

- log files
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [12](#)

M

- manage file types
 - VirusScan Enterprise for NetApp [11](#)
 - VirusScan Enterprise for ICAP [14](#)
- manage ICAP servers [14](#)
- memory requirements [7](#)

N

- NetApp
 - filers [4](#)
 - upgrading 7.1 to VirusScan Enterprise for Storage 1.0 [8](#)
- Network Appliance Filers tab, VirusScan Enterprise for NetApp NetApp [11](#)

O

- Online Help [4](#)
- operating systems, supported [7](#)

P

- Performance tab
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [12](#)
- port numbers, VirusScan Enterprise for ICAP [14](#)
- pre-installation [6](#)
- processor requirement [7](#)

R

- Release Notes [4](#)
- Reports tab
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [12](#)

S

- Scan Items tab
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [11](#), [12](#)
- settings
 - VirusScan Enterprise for ICAP [14](#)
 - VirusScan Enterprise for NetApp [12](#)
- system requirements [7](#)